Appendix M - Glossary

Accreditation

The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Alpha testing

Includes functional testing and dry-run security testing usually performed in the contractor's facility

Availability

Timely, reliable access to data and information services for authorized users

Beta 1

Security certification testing performed in a lab environment or other facility as appropriate

Beta 2

Security certification testing performed at designated operational installation(s) until stable baseline is achieved (configuration differences or other factors may necessitate multiple Beta 2 test sites)

Certification

The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes.

Controlled Interface

A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system)

Data Owner

The organization that has final statutory and operational authority for specified information.

Designated Accrediting Authority (DAA)

Official with authority to formally assume responsibility for operating a system at an acceptable level of risk

DExA for T&E

DoDIIS Executive Agent for Test and Evaluation—497th Intelligence Group/INDS

IC Panel/Board

Per DCID 6/3, refers to the Defense and Intelligence Community Accreditation Support Team (DICAST)

Independent Validation and Verification (IV&V)

An evaluation of the security features of the system by an organization(s) not responsible for the development of the system. An IV&V team is required for PL4 and PL5 systems.

Information Assurance

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information System (IS)

Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); includes software, firmware, and hardware.

Information System Security Manager (ISSM)

The manager responsible for an organization's information system security program.

Information System Security Officer (ISSO)

The person responsible to the ISSM for ensuring that operational security is maintained for a specific IS, sometimes referred to as a Network Security Officer.

Integrity

Protection against unauthorized modification or destruction of information.

Interconnected System

A set of separately-accredited systems that are connected together.

Joint Accreditation

An accreditation process that is required when an IS is not under the sole jurisdiction of a single accrediting authority.

Least Privilege

The principle requiring that each subject is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

Level-of-Concern

The Level-of-Concern is a rating assigned to an IS by the DAA. A separate Level-of-Concern is assigned to each IS for confidentiality, integrity, and availability. The Level-of-Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level-of-Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits. The Level-of-Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level-of-Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Memorandum of Agreement (MOA)

A written agreement among the DAAs responsible for the information processed and maintained by an IS (or collection of ISs). The MOA stipulates all of the terms and conditions of the security arrangements that will govern the operation of the IS(s). The MOA shall include at least: (1) a general description of the information to be offered by each participating DAA; and (2) a discussion of all of the security details pertinent to the exchange of information between the DAAs. In addition, where the MOA is to cover an interconnected network of ISs of under the purview of different DAAs, then the MOA shall also include a description of the types of information services each participating IS will provide, and identify a lead DAA. If no lead DAA is named, then both parties share responsibility.

Operational testing

Security certification testing performed in an operational environment (assumes stable baseline)

Penetration testing

System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain "root" or "superuser" privileges) by exploiting flaws in system design or implementation. It is the portion of security testing that attempts to circumvent the security features of the system—may be accomplished via NSA profiling or by DIA Operations and Assessment Team. The Program Management Office (PMO) is responsible for coordinating profiling activity with NSA and DIA.

Principal Accrediting Authority (PAA)

Senior official having authority and responsibility for all intelligence systems within an agency

Protection Level

An indication of the implicit level of trust that is placed in a system's technical capabilities. A Protection Level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review.

Risk

The expected loss from a given attack or incident. For an attack/defense scenario, risk is assessed as a combination of threat (expressed as the probability that a given action, attack or incident will occur, but may also be expressed as frequency of occurrence), vulnerability (expressed as the probability that the given action, attack, or incident will succeed, given that the action, attack or incident occurs) and consequence (expressed as some measure of loss, such as dollar cost, resources cost, programmatic impact, etc.). The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by countermeasures.

Risk Assessment

The process of analyzing the threats to and vulnerabilities of an information system, analyzing the potential impact that the loss of information or capabilities of a system would have on national security, and, based upon these analyses, identifying appropriate and cost-effective counter-measures.

Risk Management

The discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level.

Residual Risk

Portion of risk that remains after security measures have been applied.

Security Certification Letter

Documents results of Beta 1 and Beta 2 security certification testing for Intelligence Mission Applications

Sensitive Compartmented Information

Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19).

Sensitive Compartmented Information Facility (SCIF)

An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed (DCID 1/19).

Stable Baseline

The system baseline is considered stable when there are minimal security findings (no Category I findings), the system is under configuration control, and has been accepted operationally

System Security Authorization Agreement (SSAA)

Document describing the necessary protections to allow the system to operate securely. A sample SSAA outline is described in Annex 1.

Trusted Facility Manual

The document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.

Virtual Test Folder

A web site maintained by the DoDIIS Joint Integration Test Facility (JITF) containing test process information, including test plans, test reports and other information, for DoDIIS Intelligence Mission Applications

Vulnerability assessment testing

The portion of security testing conducted to ensure the system configuration does not contain any well-known security vulnerabilities